NASA Procedural Requirements

NPR 8000.4A
Effective Date: December 16, 2008
Expiration Date: December 16, 2013

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Agency Risk Management Procedural Requirements

Responsible Office: Office of Safety and Mission Assurance

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

Chapter 1. Introduction

1.1 Background

1.1.1 General

a. Generically, risk management is a set of activities aimed at achieving success by proactively risk-informing the selection of decision alternatives and then managing the implementation risks associated with the selected alternative. In this document, risk management is defined in terms of RIDM and CRM. The document addresses the application of these processes to the safety, technical, cost, and schedule mission execution domains throughout the life cycle of programs and projects, including acquisition. In addition, institutional risks and the coordination of risk management activities across organizational units are addressed.

b. The purpose of integrating RIDM and CRM into a coherent framework is to foster proactive risk management: to better inform decision making through better use of risk information, and then to more effectively manage implementation risks using the CRM process, which is focused on the baseline performance requirements emerging from the RIDM process. Within an RIDM process, decisions are made with regard to outcomes of the decision alternatives, taking into account applicable risks and uncertainties; then, as part of the implementation process, CRM is used to manage those risks in order to achieve the performance levels that drove the selection of a particular alternative. Proactive risk management applies to programs, projects, and institutional or mission support offices. Correspondingly, the requirements within this NPR are broadly applicable to these areas. Figure 1 shows where the specific processes from the discipline-oriented NPR 7123.1 and NPR 8000.4 intersect with product-oriented NPRs, such as NPR 7120.5D, NPR 7120.8, and NPR 7120.7. In much the same way that NPR 7123.1 is intended to define specific systems engineering processes that work within program and project contexts, this NPR is intended to define a risk management process in a manner that can be applied within the various contexts.

c. This NPR supports NASA's internal control activities as specified in NPD 1200.1, which implements Office of Management and Budget Circular A-123 (Management's Responsibility for Internal Control) and the related Government Accountability Office Standards for Internal Control in the Federal Government. This NPR establishes the framework for conducting risk management across programmatic, financial, and institutional activities. These risk management activities provide a basis for establishing internal controls to mitigate the identified risks. The effectiveness of the internal controls is assessed and reported in accordance with the requirements contained in NPD 1200.1.

d. This NPR is intended to be applied and implemented within the organizational structure of the activity being performed. It is not intended to dictate that organizational structure.

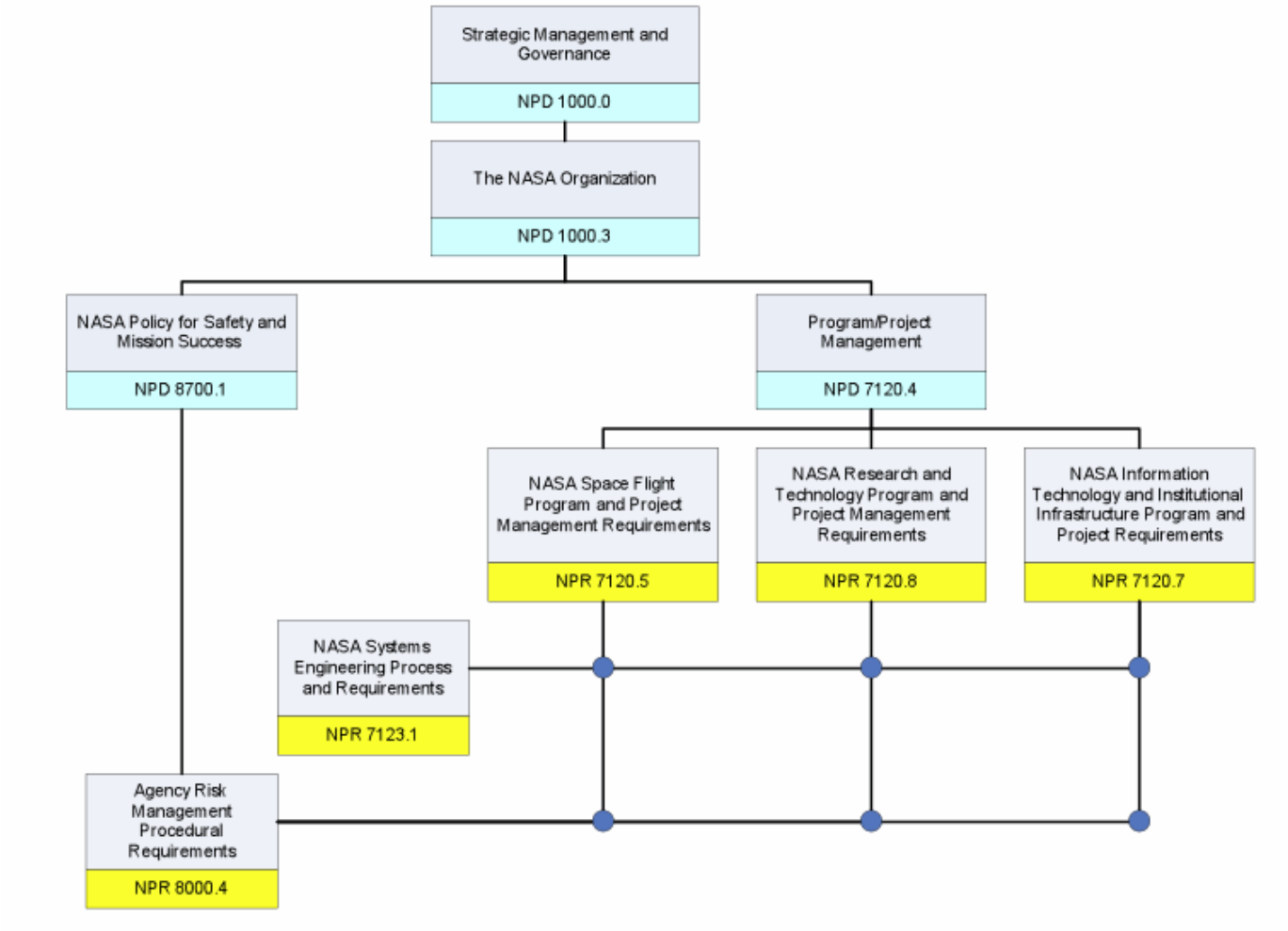

Figure 1. Intersection of Discipline-Oriented and Product-Oriented NPRs

1.1.2 Precedence

The order of precedence in cases of conflict among requirements is 42 U.S.C. 2473(1), Section 203(1), National Aeronautics and Space Act of 1958, as amended; NPD 1000.0, Governance and Strategic Management Handbook; and NPD 1000.3, The NASA Organization.

1.1.3 Requirement Verbs

In this NPR, a requirement is identified by "shall," a good practice by "should," permission by "may" or "can," expected outcome or action by "will," and descriptive material by "is" or "are" (or another form of the verb "to be").

1.1.4 Figures

The figures within this NPR are intended to be illustrative, not prescriptive.

1.2 Risk Management Within the NASA Hierarchy

1.2.1 Key Concepts

a. In the context of mission execution, risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements. The performance shortfalls may be related to institutional support for mission execution or related to any one or more of the following mission execution domains:

(1) Safety

(2) Technical

(3) Cost

(4) Schedule

b. In this document, the term "Performance Measure" is defined generically as a metric to measure the extent to which a system, process, or activity fulfills its intended objectives. Performance Measures for mission execution may relate to safety performance (e.g., avoidance of injury, fatality, or destruction of key assets), technical performance (e.g., thrust or output, amount of observational data acquired), cost performance (e.g., execution within allocated cost), or schedule performance (e.g., meeting milestones). Similar performance measures can be defined for institutional support.

c. NASA's decisions for managing risk involve characterization of the three basic components of risk:

(1) The *scenario(s)* leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage);

(2) The *likelihood(s)* (qualitative or quantitative) of those scenario(s); and

(3) The *consequence(s)* (qualitative or quantitative severity of the performance degradation) that would result if the scenario(s) was (were) to occur.

Note 1: "Likelihood" is a measure of the possibility that a scenario will occur, which accounts for the frequency of the scenario and the timeframe in which the scenario can occur. For some purposes, it can be assessed qualitatively. For other purposes, it is quantified in terms of frequency or probability.

Note 2. A complete characterization of the scenarios, likelihoods, and consequences also calls for characterization of their uncertainty.

d. Each organizational unit will oversee the risk management processes of those unit(s) at the next lower level, as well as manage risks identified at its own level. In most cases, an organizational unit, at a given level, within NASA negotiates with the unit(s) at the next lower level in the organizational hierarchy a set of objectives, deliverables, performance measures, baseline performance requirements, resources, and schedules that defines the tasks to be performed by the unit(s). Once established, the lower level organizational unit manages its own risks against these specifications, and, as appropriate, reports risks and elevates decisions for managing risks to the next higher level based on predetermined risk thresholds (illustrated below) that have been negotiated between the two units. Figure 2 depicts this concept. Risk management decisions are elevated by an organizational unit when those risks can no longer be managed by that unit. This may be the case if, for example, resources are not available, or the organizational unit lacks the decision authority needed in order to manage those risks. In many cases, elevation needs to occur in a timely fashion, in order to allow upper management to respond effectively. The approach is performance-based in the sense that each unit determines the best way to achieve its objectives and performance requirements, rather than being told in detail how these are to be achieved. Risk management decisions may be elevated beyond the next higher level, but it is assumed that a risk management decision is elevated through a stepwise progression. This discussion applies to the risk management process, not to other Agency processes that govern the handling of dissenting opinions or safety concerns.

Note: The relationships between a performance requirement, risks, and associated thresholds can be illustrated using the following example. Suppose that for development of a particular science module, a "mass" performance measure has a baseline performance requirement of 50 kg. Lower mass is preferred; mass significantly greater than 50kg has not been allowed for. The risk associated with this technical performance measure is characterized in terms of one or more scenarios leading to higher mass, their associated likelihoods, and the severity of the associated mass exceedance in each case. A threshold for elevation might be established probabilistically; e.g., as a specified probability (P) of exceeding the baseline mass requirement (50 kg in this case).

e. Mission Directorates are responsible for management of programmatic risks within their domains and are responsible for elevating risks to the Management Councils (Program Management Council, Operations Management Council, and Strategic Management Council) at the Agency level as appropriate. Center Directors are responsible for management of institutional risks at their respective Centers. Headquarters Mission Support Offices are responsible for management of Agency-wide institutional risks. Program and project managers are responsible for program and project risks within their respective programs and projects. Refer to Chapter 2 for a full description of roles and responsibilities.

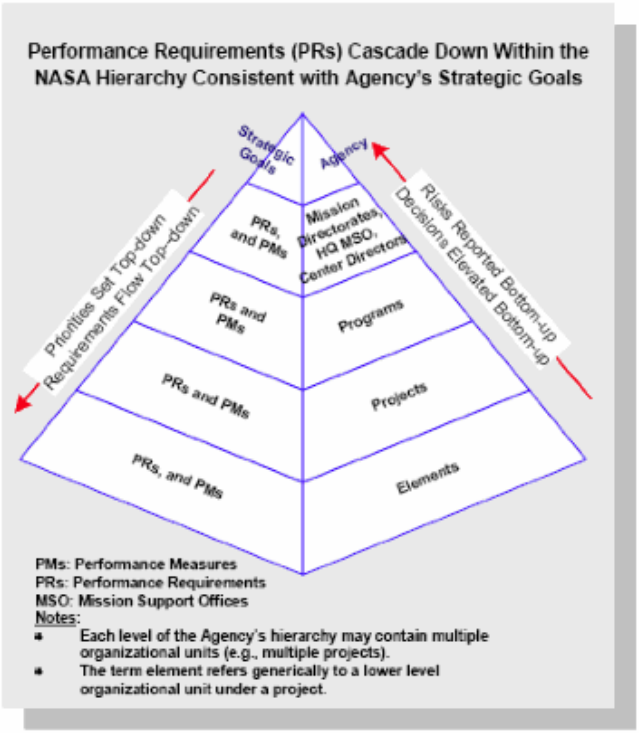

Figure 2. Flowdown of Performance Requirements (Illustrative)

f. Risk management at the Agency level addresses risks identified at the Agency level, as well as risks elevated from Mission Directorates and Mission Support Offices. These risks may have been elevated for any of several reasons, including:
(1) A need for the Agency to allocate additional resources for effective mitigation.
(2) Agency-level coordination/integration is needed with other organizations/stakeholders.
(3) A finding that a risk identified within a directorate is, in fact, an Agency-level concern.
g. Risk management at the Agency level integrates the full spectrum of risks.
(1) Dealing with risk as a strategic issue, from a high Agency-level/corporate perspective.
(2) Engaging all functions and line management levels in the process.
(3) Bridging the gaps between domains of risk management (e.g., safety, technical, financial/cost, institutional).
h. At the Agency level, emphasis is placed on optimizing and improving the Agency's mission objectives and goals versus individual project or program goals/objectives. Per NPD 1000.0, this is carried out by the Agency's Management Councils.

1.2.2 RIDM

a. As shown in Figure 3, RIDM within each organizational unit involves:

(1) Identification of decision alternatives, recognizing opportunities where they arise, and considering a sufficient number and diversity of performance measures to constitute a comprehensive set for decision-making purposes.

(2) Risk analysis of decision alternatives to support ranking.

(3) Selection of a decision alternative *informed by* (not solely based on) risk analysis results.

b. RIDM is conducted in many different venues based on the management processes of the implementing organizational unit. These include boards and panels, Authority to Proceed milestones, Safety Review Boards, Risk Reviews, Engineering Design and Operations Planning decision forums, Configuration Management processes, and commit-to-flight reviews, among others.

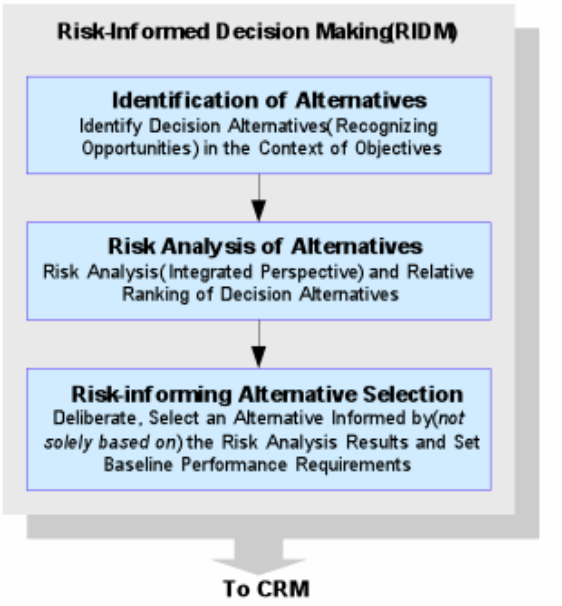

Figure 3. RIDM Process

c. As part of a risk-informed process, the complete set of performance measure values (and corresponding assessed risks) is used, along with other considerations, within a *deliberative* process to improve the basis for decision making. Deliberation helps the organization to make the best possible use of its experience and tacit knowledge. For example, in order to inform decisions that affect safety, safety performance measures (such as crew safety) and related risks (such as contributions to the probability of loss of crew due to micrometeoroid impact) can be considered in light of aspects of performance history that are not captured in the risk models.

d. Once a decision alternative has been selected for implementation, the performance measure values that informed its selection define the baseline performance requirements for CRM. As discussed in paragraph 1.2.4.f, situations may arise in which it is necessary to revisit the decision and rebaseline the performance requirements.

e. In order to focus effort and accountability during implementation of the selected alternative, CRM may focus on a set of individual risk contributors (i.e., specific "risks"). However, for some purposes, decision making needs to be supported by quantification of the "aggregate risk" associated with a given performance measure; i.e., aggregation of all contributions to the risk associated with that performance measure. For example, it may not be sufficient to consider only a list of "risks" to the crew of a human-crewed space vehicle; in order to support some decisions, it is necessary to quantify the total probability of loss of crew, considering all contributions, as an aggregated risk. Similarly, cost risk is usually treated in the aggregate. For some performance measures, it may not be practical to quantify the aggregate risk; the feasibility of quantifying aggregate risk is determined for each performance measure and then documented in the Risk Management Plan (see paragraph 3.1.2) for each organizational unit.

1.2.3 CRM

a. NASA uses a specific process for the management of risks associated with implementation of designs, plans, and processes. This process, which is represented by the graphic in Figure 4 below, is referred to as CRM.

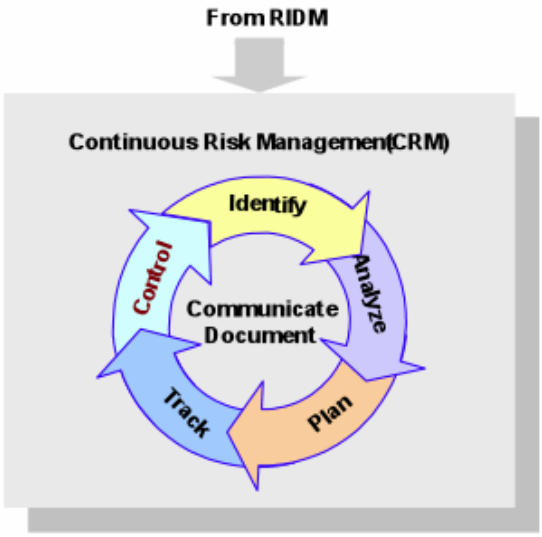

Figure 4: CRM Process

b. Steps in the CRM process include:

(1) Identify: *Identify* contributors to risk (shortfalls in performance relative to the baseline performance requirements).

Note: Sometimes the relationship between an identified risk and performance measures is indirect, but risks within the proper scope of CRM are addressed precisely because they may affect one or more performance measures.

(2) Analyze: Estimate the probability and consequence components of the risk through *analysis*, including uncertainty in the probabilities and consequences and, as appropriate, estimate aggregate risks.

(3) Plan: Decide on risk disposition and handling, develop and execute mitigation *plans*, and decide what will be tracked.

(4) Track: *Track* observables relating to performance measures (e.g., technical performance data, schedule variances).

(5) Control: *Control* risk by evaluating tracking data to verify effectiveness of mitigation plans, making adjustment to the plans as necessary, and executing control measures.

(6) Communicate and document: *Communicate and document* the above activities throughout the process.

1.2.4 Coordination of RIDM and CRM Within and Across Organizational Units

a. The right-hand portion of Figure 5 shows RIDM (previously shown in Figure 3) and CRM (previously shown in Figure 4) as complementary processes that operate within every organizational unit. Each unit applies the RIDM process to decide how to fulfill its performance requirements and applies the CRM process to manage risks associated with implementation.

b. The left portion of Figure 5 (previously shown in Figure 2) shows the hierarchy of organizations tasked with carrying out a mission. At any given level below the Agency level, there may be multiple organizational units conducting RIDM and CRM. Associated coordination activities include flowdown of performance requirements, risk reporting, and elevation of decisions. Coordination of risk management is suggested by Figure 5. This coordination enables the optimum flow of risk information at all levels of the Agency.

Note: Tools of Knowledge Management (KM) are expected to be particularly valuable in this regard.

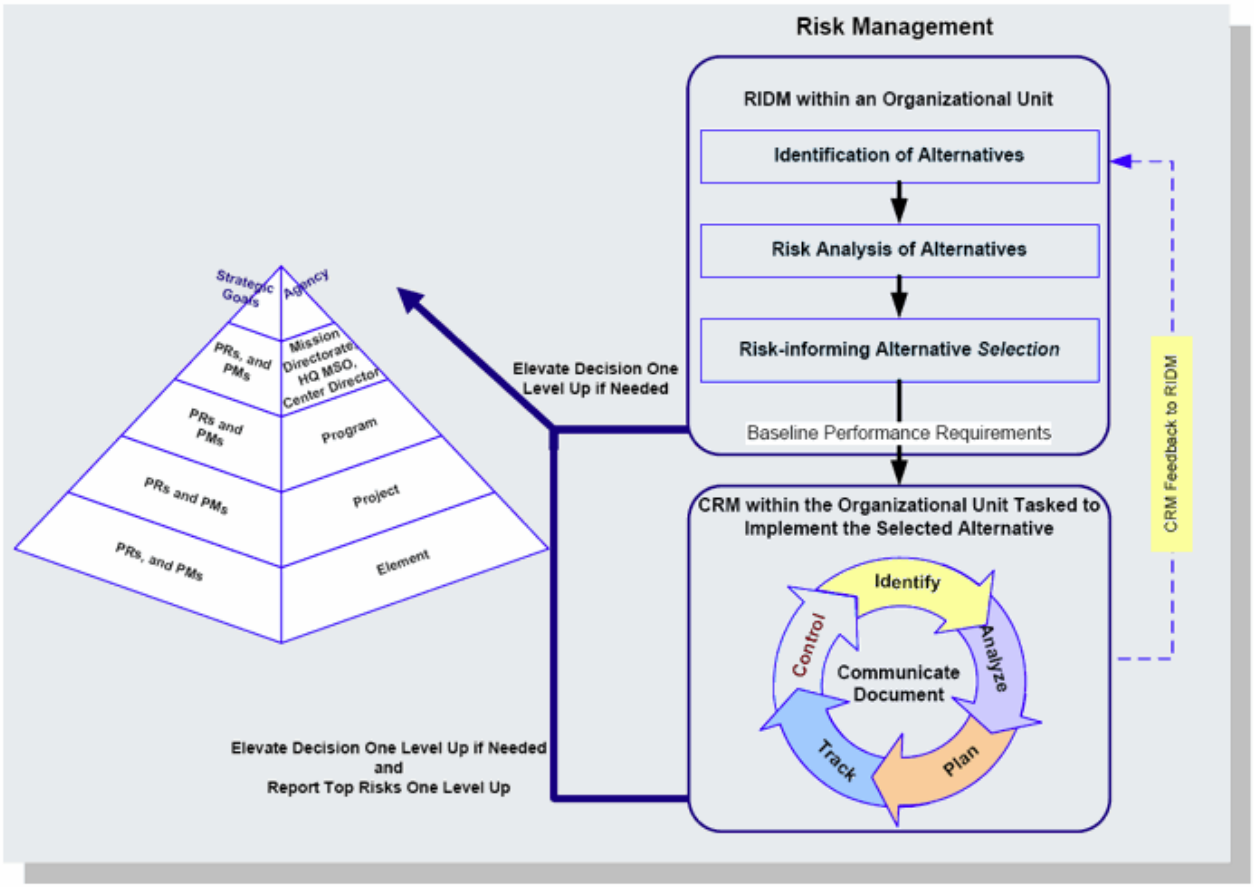

Figure 5. Coordination of RIDM and CRM Within the NASA Hierarchy (Illustrative)

c. Each organizational unit reports on its risk management activities to the sponsoring organization at the next higher level and may elevate individual risk management decisions to that level, if it is determined that those risks cannot be addressed by the originating unit. Refer to paragraph 1.2.1.

d. Within each organizational unit, disposition of risks includes the use of defined thresholds whose exceedance should initiate a risk control response by the unit, including the possible elevation of risk management decisions to the sponsoring organization at the next higher level (as discussed in paragraph 1.2.1d). The Risk Management Plan articulates decision rules for dispositioning individual and aggregate risks, including the consideration of uncertainties in the decision process.

e. Satisfaction of performance requirements needs to be demonstrated by the lower level organizational unit to the upper level through periodic reporting of the status of risks associated with each performance measure. A basis for the evaluation of the performance measures and their associated risks should be agreed upon and documented in advance (or indicated by reference) in the Risk Management Plan (see paragraph 3.1.2.c).

f. It is the responsibility of the organizational unit at the higher level to assure that the performance requirements assigned to the organizational unit at the lower level reflect appropriate tradeoffs between/among competing objectives and risks. It is the responsibility of the organizational unit at the lower level to establish the feasibility of managing the risks of the job it is accepting, including identification of mission support requirements. The performance requirements can be changed, if necessary, but redefining and rebaselining them need to be negotiated with higher levels, documented, and subject to configuration control. Performance requirements work together, so redefinition and rebaselining one performance requirement may force redefinition and rebaselining of another, if the overall program/project objectives are to be satisfied. Redefinition and rebaselining, therefore, imply a tradeoff that is the responsibility of the higher level.

g. Both CRM and RIDM are applied within a graded approach. The resources and depth of analysis need to be commensurate with the stakes and the complexity of the decision situations being addressed. For example, the level of rigor needed in risk analysis to demonstrate satisfaction of safety-related performance requirements depends on specific characteristics of the situation: how stringent the requirements are, how complex and diverse the hazards are, and how large the uncertainties are compared to operating margin, among other things. Both RIDM and CRM are formulated to allow for this.

h. At each Center, management of institutional risks affecting multiple programs/projects is carried out within Center organizational units. These units are distinct from the program/project units. Analogously to lower-level program/project organizational units, support organizations receive requirements from, and report risks to, the organizational units that they support. However, management of institutional risks is done within the Center support hierarchy and coordinated with the program/project organizational units as needed. Since the program/project organizational units are affected by institutional risks without being in a position to manage them proactively, in the event that institutional risks threaten accomplishment of program/project organizational unit performance requirements, the program/project organizational units need either to manage those risks with their own resources or elevate them to the next level within the program/project hierarchy.

i. Agency-wide institutional risks are addressed by NASA Headquarters Mission Support Offices and the Operations Management Council.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS